



Department of Homeland Security Information Analysis and Infrastructure Protection Daily Open Source Infrastructure Report for 04 February 2004

Current Nationwide
Threat Level is



[For info click here](#)

www.whitehouse.gov/homeland

Daily Overview

- WNEP News reports the chemical reaction from leaking tanker on Interstate 80 in Pennsylvania forced the evacuation of about 1,000 nearby residents. (See item [3](#))
- The Associated Press reports a security company with contracts to protect New York–area airports, bridges and tunnels has been charged with paying bribes to get work and hiring employees with criminal records. (See item [8](#))
- The Associated Press reports a white powder found in Senate Majority Leader Bill Frist's office Tuesday, February 2, tested as an "active" form of the poison ricin, forcing cancellation of most Senate business. (See item [10](#))

DHS/IAIP Update *Fast Jump*

Production Industries: [Energy](#); [Chemical](#); [Defense Industrial Base](#)

Service Industries: [Banking and Finance](#); [Transportation](#); [Postal and Shipping](#)

Sustenance and Health: [Agriculture](#); [Food](#); [Water](#); [Public Health](#)

Federal and State: [Government](#); [Emergency Services](#)

IT and Cyber: [Information and Telecommunications](#); [Internet Alert Dashboard](#)

Other: [General](#); [DHS/IAIP Web Information](#)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES-ISAC) – <http://esisac.com>]

1. ***February 03, Oil Online*** — Alyeska pipeline project upgrades monitoring system. Alyeska Pipeline Service Company has broken away from the traditional pipeline SCADA systems and turned to a newer, more efficient technology called UCOS Pipeline SCADA. Alyeska is installing UCOS as the primary SCADA Master Station and Data Historian for the trans-Alaskan Pipeline. UCOS (User Configurable Open Systems) applies object-oriented programming and user interface techniques, executes on standard, off-the-shelf hardware, and

can be integrated with existing field equipment that often requires no rewiring. **When the Alyeska project is completed, UCOS will provide instantaneous monitoring and control of all significant aspects of operations, including monitoring the pipeline's leak detection system.** Operators using real-time dynamic graphic displays monitor the system 24-hours a day and control oil movement through the pipeline and tanker loading.

Source: http://www.oilonline.com/news/headlines/firms_faces/20040203_Alyeska_13499.asp

2. *February 03, PRNewswire* — **Credit card scam affecting utility customers. Pacific Gas and Electric Company is warning its customers to beware of telephone calls from anyone claiming to be from Pacific Gas and Electric Company and asking for credit card information.** The company has received reports from customers throughout its California service area about an alleged telephone scam. The caller claims to be from PG&E and threatens to shut off gas and electric service if the customer does not provide a credit card number to pay the bill. This same scenario has been reported in Bakersfield and Eureka, with the latest incident occurring on Friday to a customer in San Jose. While PG&E offers several payment options, it does not accept credit cards for payment of energy bills.

Source: http://biz.yahoo.com/prnews/040203/sftu088_1.html

[[Return to top](#)]

Chemical Sector

3. *February 03, WNEP News (PA)* — **Chemical spill leads to investigation.** It should not have happened! That's what a fire chief said about a leaking tanker that caused some chemical confusion in Columbia County (PA) Monday night, February 2. It led to an evacuation, an interstate closing and now an investigation. **The tanker held thousands of gallons of three different acids. When it began to leak along Interstate 80 near Mifflinville, a cloud formed overhead. The chemical reaction forced the evacuation of about 1,000 nearby residents. They had to stay away for at least six hours.** "This was approved hauling and approved in the mixture they had. Somewhere something went wrong and created the reaction that created this situation and that's been undetermined yet," explained Mifflinville Fire Chief Don Diltz. What went wrong is under investigation by the state and the trucking company. Some suspect the three acids reacted with something else in the tanker that heated the side of the container to 210 degrees. Fire officials said Tuesday because of the amount of traffic on the interstate, this could and most likely will happen again.

Source: <http://www.wnep.com/Global/story.asp?S=1628753&nav=5ka4Kasg>

[[Return to top](#)]

Defense Industrial Base Sector

4. *February 01, National Defense Magazine* — **Army to upgrade land warrior system with blue-force tracker.** In response to feedback from soldiers in Iraq, the Army intends to add blue-force tracking capabilities to a handheld computer that is being developed for the Land Warrior program. The battle-management computer, called the Commander's Digital Assistant (CDA), was designed to help battalion and company commanders, as

well as platoon leaders, maintain "situational awareness" of their troops as they move around the battlefield. Land Warrior also is part of an ambitious long-term plan to connect dismounted troops into tactical networks. The next step in the evolution of Land Warrior, said program officials, is to combine the CDA technology with the blue-force tracking device widely used in Operation Iraqi Freedom—the Force XXI Battle Command Brigade and Below, or FBCB2. One key feature that the Army wants in the CDA is L-band satellite connectivity, which is available in FBCB2. Lt. Col. David Gallop, Army program manager for Land Warrior, said it would not be unreasonable to expect the L-band upgrade and the blue-force tracking capability in CDA by April. The long-term goal is to provide T-1 encryption, which is the highest level. Current CDAs have T-3 encryption.

Source: <http://nationaldefense.ndia.org/article.cfm?Id=1339>

[\[Return to top\]](#)

Banking and Finance Sector

5. *February 03, Korea Times* — **Korea to toughen money laundering law. Starting in the latter half of next year, banks and other financial services institutions in (South) Korea will be required to report to the authorities all cash transactions of US\$42 million or more.** Currently, banks and financial services companies are required to submit information only when transactions over that amount are deemed suspicious. The Korea Financial Intelligence Unit (KoFIU) announced on Tuesday that it would push for a revision of the related law within the year. "The new regulation will only take effect from next June, because it takes about a year to computerize the networks," KoFIU Commissioner Kim Byung-ki said. Source: http://times.hankooki.com/lpage/biz/200402/kt200402031815111_1910.htm

[\[Return to top\]](#)

Transportation Sector

6. *February 03, Department of Transportation* — **Secretary Mineta recommends key transit projects for federal funding.** The U.S. Department of Transportation yesterday, February 2, recommended to Congress more than \$1.5 billion in funding for 34 new or expanding urban and suburban transit programs **aimed at improving job access and increasing commuter mobility in major cities like Cleveland, New York, Phoenix and others around the country.** This year's FY 2005 recommendations include 34 current or pending transit projects, such as the creation of a major, 35 station Bus Rapid Transit zone in Cleveland; an extension of New York's Long Island Rail Road that will increase access into and out of Manhattan and Queens; and a new 20-mile light rail system in Phoenix connecting commuters from the Spectrum Mall to several of the area's central business districts, Sky Harbor Airport and professional sports venues. Transportation Secretary Norman Y. Mineta said that transit projects represent key economic investments that will help several of the country's most populated cities improve job access, increase mobility and ease congestion. **When completed, these projects are expected to carry over 243 million commuters each year, while saving over 121 million hours in potential travel delays and significantly improving air quality in many of our nation's most congested cities.**

Source: <http://www.dot.gov/affairs/fta204.htm>

7. *February 03, Hawaii Tribune–Herald* — **Missing air ambulance located. The wreckage of a missing air ambulance and the bodies of three crewmen who were aboard the Hilo, (HI) bound plane were found Monday morning, February 2, about 4.5 miles above Ookala.** The Coast Guard at 9:48 a.m. picked up a faint signal from the electronic locating transmitter carried by the Cessna missing since early Saturday, Petty Officer Jennifer Johnson said. After receiving the coordinates of the wreckage, Hawaii County rescue personnel flew to the wooded area located at the 3,600 – foot level of Mauna Kea, Capt. Clint Coloma said. There were no survivors. **The FAA and the National Transportation Safety Board are investigating.**
Source: <http://www.hilohawaiitribune.com/daily/2004/Feb-03-Tue-2004/news/news1.html>

8. *February 03, Associated Press* — **Airport security company accused of bribery.** A security company with contracts to protect New York–area airports, bridges and tunnels has been charged with paying bribes to get work and hiring employees with criminal records. **Haynes Security Inc. and its president, John D'Agostino, were charged with theft, bribery and conspiracy in an indictment announced Tuesday, February 3.** Among the allegations: Haynes paid more than \$1,000 in August 2001 for repairs at the home of a Continental Airlines manager in return for consideration for a contract at the Newark airport. No charges were brought against any Continental employees. **The security company was also accused of failing to submit employee fingerprints to police as required by law.** Since 1999, Haynes has held \$12 million in annual contracts to provide security at Newark, Kennedy and LaGuardia airports in New York, as well as the Holland and Lincoln tunnels and the George Washington Bridge. Haynes no longer handles airport passenger screening, which is now overseen by the federal Transportation Security Administration. But the company's unarmed guards still provide security in other parts of the airports. **Investigators said Haynes hired convicted criminals — who are barred from holding security posts — to work at the airport and for the state's largest utility, Public Service Electric & Gas.**
Source: <http://www.newsday.com/business/nationworld/wire/sns-ap-secu-rity-company-bribery,0,2263235.story?coll=sns-ap-business-headlines>

9. *February 03, Singapore Business Times* — **MPA urges extra alert against pirate attacks.** Against the backdrop of rising pirate attacks in regional waters, the Maritime and Port Authority (MPA) of Singapore has strongly urged the shipping community to be extra vigilant to ensure their vessels' safety and the safety of navigation in the busy straits. **In an unusual move, the MPA issued the warning following two consecutive sea robberies three hours apart on January 29 in the eastbound lane of the Traffic Separation Scheme (TSS) of the Singapore Strait off the northeast coast of Indonesia's Karimun Island.** The MPA estimates that nearly 400 vessels a day transit that particular spot in the strait. The MPA referred the shipping community to the International Maritime Organization's MSC Circular 623/Rev.3 for guidance on anti–piracy plans.
Source: <http://business-times.asia1.com.sg/story/0,4567,106991,00.html>

[[Return to top](#)]

Postal and Shipping Sector

10. *February 03, Associated Press* — **Ricin find stops most Senate business. A white powder found in Senate Majority Leader Bill Frist's office tested Tuesday as an "active" form of the poison ricin, forcing cancellation of most Senate business.** But officials have found no evidence that anyone was significantly exposed to the poison enough "to make them sick, said Dr. John Eisold, the Capitol physician. Frist said that tests confirmed that the powder was ricin: "It is active, how active we don't know." He said he was confident that everyone who was at risk has been identified. **U.S. Capitol police chief Terrance Gainer said everything that was in the 4th floor mailroom in Frist's Dirksen Senate Office Building office has been seized, but that authorities have not yet analyzed all of the mail.**

Source: http://story.news.yahoo.com/news?tmpl=story&cid=519&e=1&u=/ap/20040203/ap_on_re_us/capitol_ricin

11. *February 03, Reuters* — **Suspicious gray granules found in Connecticut mail. An envelope containing a suspicious powder found in a Connecticut post office overnight was addressed to the Republican National Committee and is being tested to see if it is the poison ricin, officials said on Tuesday.** Officials in Connecticut said field tests of the powder were inconclusive but all mail associated with the envelope was isolated until laboratory tests were completed later on Tuesday. "We are performing a battery of tests for biological and chemical agents including testing for the presence of ricin," Connecticut health department spokesman Michael Purcaro said. The envelope leaking grayish, sandy granules was found in Wallingford, CT, in one of the same mail sorting facilities where anthrax bacteria spores were found in the 2001 anthrax attacks.

Source: <http://www.alertnet.org/thenews/newsdesk/N03388023.htm>

[\[Return to top\]](#)

Agriculture Sector

12. *February 03, Vietnam News Agency* — **Indonesia confirms bird flu outbreak. Indonesia's Director for Animal Health Department of the Agriculture Ministry Tri Satya Naipospos on Tuesday officially confirmed the presence of the bird flu outbreak in the country.** Java and Bali islands were reported to be hard hit by the outbreak. Farmers on these islands have killed 15 million chickens. In an effort to curb the spread of the outbreak, the Indonesian government pledged to spend more than \$25 million in culling infected fowls and buying vaccines.

Source: http://www.vnagency.com.vn/NewsA.asp?LANGUAGE_ID=2&CATEGORY_ID=33&NEWS_ID=40909

13. *February 01, Associated Press* — **Cattle TB detected in Texas. A herd of dairy cattle in Central Texas has tested positive for cattle tuberculosis (TB), state officials said. The infection at a Hamilton County dairy is the first discovered through a statewide testing program launched in November, the Texas Animal Health Commission said in a statement.** Veterinarians have tested 57 purebred herds and 82 dairies since the program began, the commission said. They plan to test about 2,400 of the state's seedstock beef herds and all of Texas' 831 dairy herds before September 2004 as part the federally funded surveillance program. **Officials are trying to determine how the herd was infected and if the infection has spread to other herds.** TB is highly contagious among cattle, causing abscesses and

leading to death, but it cannot be spread to humans. The Hamilton County dairy was quarantined by the agency in late December, after a number of animals reacted to TB skin tests, said Bob Hillman, Texas' state veterinarian. Veterinarians collected tissue from several of the dairy animals and forwarded the samples to the National Veterinary Services Laboratory in Ames, IA.

Source: <http://www.landandlivestockpost.com/livestock/020104tb.htm>

[\[Return to top\]](#)

Food Sector

14. *February 03, Food and Drug Administration* — **FDA's budget proposal requests increase for food safety.** The Food and Drug Administration (FDA) announced Tuesday, February 3, that it is seeking an increase of \$65 million for fiscal year (FY) 2005 to boost its food security activities as part of a new interdepartmental program for the defense of the Nation's food supply. **The largest part of the increase, \$35 million, would be used to increase the FDA's analytic surge capacity for biological, chemical, and radiological threat agents by enhancing the Food Emergency Response Network (FERN).** Once completed, FERN will encompass a nationwide network of Federal and State laboratories capable of testing the safety of thousands of food samples, thereby enhancing the Nation's ability to swiftly respond to a terrorist attack. **Fifteen million of the \$65 million increase is proposed to fund research on prevention technologies, methods development, and determination of infectious dose for potential terrorism agents when ingested with food, and identification of agent characteristics within specified foods.** Another \$7 million is earmarked for increased FDA inspections of domestic and imported food. An additional \$3 million of the proposed increase is to be used to upgrade the agency's crisis management by boosting its capacity for rapid and coordinated response to a threat to the the food supply.

Source: <http://www.fda.gov/bbs/topics/NEWS/2004/NEW01015.html>

[\[Return to top\]](#)

Water Sector

Nothing to report.

[\[Return to top\]](#)

Public Health Sector

15. *February 03, Boston Globe* — **Researchers identify a SARS antibody. Researchers at the Dana–Farber Cancer Institute in Boston, MA, announced yesterday that they have identified a human antibody that powerfully blocks infection by the Severe Acute Respiratory Syndrome (SARS) virus.** The discovery could lead to a new treatment that could be tested on humans in as little as a year. Scientists identified the antibody 80R by systematically scanning a 27–billion antibody "library," looking for antibodies that specifically targeted SARS, chemically bonding with them and preventing them from entering healthy cells. The team, working with researchers from Brigham and Women's and Boston Children's

hospitals as well as the U.S. Centers for Disease Control and Prevention, found that 80R prevented the virus from entering healthy cells in the first place, by gumming up the machinery SARS uses to penetrate cell walls.

Source: http://www.boston.com/news/globe/health_science/articles/2004/02/03/researchers_identify_a_sars_antibody/

16. *February 03, Associated Press* — **Bird flu meeting begins in Rome. Health, food, and animal experts began an urgent meeting Tuesday to discuss the bird flu outbreak in Asia that has killed 12 people, devastated poultry farms, and raised concern that the virus could mutate into a more dangerous form.** The UN Food and Agriculture Organization (FAO) is hosting the three-day meeting at its Rome, Italy, headquarters. **The experts hope "to develop shared strategies for helping affected countries respond to the existing emergency and prevent future outbreaks of the disease," an FAO statement said.** International experts at the meeting include high-level veterinary officials from stricken countries and representatives of the U.S. Centers for Disease Control and Prevention. Although 10 countries are battling bird flu, cases in humans have been reported only in Vietnam and Thailand. FAO officials said they believe the disease is spreading within Thailand and Vietnam, but that the situation is less clear for China, where investigators may just now be picking up previously undetected cases.

Source: http://story.news.yahoo.com/news?tmpl=story&cid=541&ncid=751&e=5&u=/ap/20040203/ap_on_he_me/bird_flu

17. *February 02, Associated Press* — **Arkansas not poised to deal with bioterrorism. A new study says Arkansas is among states that would likely be vulnerable to a bioterrorism attack.** The study analyzed a whooping cough outbreak that infected more than a thousand Arkansas residents two winters ago. Gary Wheeler, director of infectious diseases at Arkansas Children's Hospital and an author of the study, says the data shows that Arkansas would face difficulty coping with a fast-spreading disease. **The report cited the difficulty in diagnosing whooping cough quickly. It said the state was hampered by many rural areas not having enough staff trained to collect specimens, and by its having a lab only at Little Rock.** Many times, Health Department contact with doctors and nurses in the field was "hit or miss." The study pointed to several areas where Arkansas could improve its response to another outbreak of an infectious disease, including better communications among healthcare professionals and more support for diagnosis in laboratories.

Source: <http://www.katv.com/news/stories/0204/123269.html>

[[Return to top](#)]

Government Sector

18. *February 03, National Journal* — **Justice Department budget centers on fighting terrorism.** Funding for the Justice Department under the Bush administration budget would grow to \$19.7 billion in fiscal 2005, from \$19.4 billion in fiscal 2004, a 2 percent increase. Justice officials emphasized the proposal's 19 percent increase in funding directed at preventing terrorist attacks, an 11.4 percent increase for the FBI and 4.5 percent for federal law enforcement programs. The total budget request is for \$22.1 billion, including mandatory spending. **The initiatives devoted to fighting terrorism include \$36 million for the Terrorism Threat**

Integration Center (TTIC) and \$29 million for the Terrorist Screening Center (TSC). TTIC is an intelligence–analysis initiative of the FBI, CIA and Homeland Security Department based at the CIA. The screening center aims to help the federal government merge terrorist watch lists. Other new programs at the FBI would include: an Office of Intelligence, a \$13 million project with 151 positions, including many consolidated from other divisions; \$14 million for a counter–terrorism headquarters support program; and \$64 million for various national security initiatives.

Source: <http://www.govexec.com/dailyfed/0204/020204tdpm1.htm>

19. *February 03, General Accounting Office* — **GAO–04–408T: Combating Terrorism: Evaluation of Selected Characteristics of National Strategies Related to Terrorism (Testimony).** Following the terrorist attacks of September 11, 2001, the Bush administration developed and published seven national strategies that relate, in part or in whole, to combating terrorism and homeland security. **In view of heightened concerns about terrorism and homeland security, General Accounting Office (GAO) was asked to identify and define the desirable characteristics of an effective national strategy and to evaluate whether the national strategies related to terrorism address those characteristics.** The purpose of this testimony is to report on GAO’s findings on this matter. GAO found considerable variation in the extent to which the seven strategies related to combating terrorism and homeland security address the desirable characteristics. **Even where the characteristics are addressed, improvements could be made.** For example, while the strategies identify goals, subordinate objectives, and specific activities, they generally do not discuss or identify priorities, milestones, or performance measures — elements that are desirable for evaluating progress and ensuring effective oversight.

Source: <http://www.gao.gov/cgi-bin/getrpt?GAO-04-408T>

[\[Return to top\]](#)

Emergency Services Sector



20. *February 03, Government Technology* — **Illinois county selects warning and messaging system.** Chairman Robert Schillerstrom and DuPage County (IL) Board unanimously approved the purchase of the EMnet system, a satellite–based warning and messaging system. This sophisticated communications system will provide secure and verifiable information during emergencies. The board has agreed to fund the purchase, installation and operating costs for the new countywide emergency warning system. **The system, the first of its kind to be utilized in Illinois, will service all municipalities in DuPage County, communicating with fire protection districts, hospitals and emergency centers. The latest in technology, the system will allow the county to coordinate information, via a secure internet link, eliminating duplicate or inaccurate messages.**

Source: <http://www.govtech.net/news/news.php?id=87075>

[\[Return to top\]](#)

Information and Telecommunications Sector

21. *February 03, Reuters* — **Microsoft site appears to weather MyDoom attack.** Microsoft Corp. appeared to have survived the worst the MyDoom worm could throw at it Tuesday. **Experts say the virus, a variant of the MyDoom.A virus that knocked out another company's Web site Sunday, was programmed to fire continuous volleys of debilitating data at Microsoft's site Tuesday. But there was no visible impact on the software company's Web site, which barely flickered as the MyDoom.B Internet worm's trigger time of 8:09 EST passed.** MyDoom.B is a low-grade variant of the original MyDoom.A virus, the fastest-spreading e-mail contagion to ever hit the Internet. MyDoom.A has infected hundreds of thousands, and possibly over one million, PCs, generating a torrent of spam e-mails and crippling corporate e-mail servers, plus slowing traffic for some Internet service providers.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=569&ncid=738&e=1&u=/nm/20040203/tc_nm/tech_microsoft_dc
22. *February 03, Government Technology* — **NTIA seeks to expand spectrum available for high-speed Internet. Last week, the National Telecommunications and Information Administration (NTIA) announced it was considering an expansion of the 3650–3700 MHz band to unlicensed devices for wireless broadband applications such as Wi-Fi while protecting federal operations in those bands from interference or other adverse effects.** NTIA has invited interested parties to file comments on technical requirements and interference-mitigation techniques necessary for compatible unlicensed device usage in those bands. "We want to make more spectrum available so that people who live in rural areas can have access to wireless broadband," said Acting Assistant Secretary of Commerce Michael D. Gallagher. "This continues our progress in facilitating the sharing of spectrum among government and commercial users." The filing says it appears that "very significant benefits" to the economy, businesses, consumers, and government agencies can be gained by allowing unlicensed devices to operate in other certain bands at higher power levels than currently permitted.
Source: <http://www.govtech.net/news/news.php?id=87078>
23. *February 02, IDG News Service* — **EU launches power line Net initiative.** Even though several high-profile companies have pulled the plug on a technology that transmits data over power lines at high speeds, the European Union (EU) hopes its support of power line communications (PLC) will help overcome technical hurdles and lead to greater competition in the broadband market. **The EU's executive arm, the European Commission, is a key sponsor of the Open PLC European Research Alliance (OPERA). The first phase, lasting two years, has a budget of \$24.8 million; it aims to develop a uniform European PLC standard.** PLC technology transmits data signals over electricity lines. While some of the early systems have delivered Internet access at speeds of up to 2Mbit/sec., others in the pipeline promise data rates of 10Mbit/sec. and higher. Although PLC competes head-on with wire-based Digital Subscriber Line and wireless LAN technologies in the local loop, the commission is particularly keen to harness the technology in order to extend broadband service in rural areas and other areas with weak infrastructures.
Source: <http://www.computerworld.com/managementtopics/outourcing/isptelecom/story/0,10801,89744,00.html>

Current Alert Levels	
 AlertCon: 2 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/
Current Virus and Port Attacks	
Virus:	#1 Virus in the United States: WORM_MYDOOM.A Source: http://wtc.trendmicro.com/wtc/wmap.html , Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	135 (epmap), 6129 (dameware), 1434 (ms-sql-m), 137 (netbios-ns), 20168 (---), 901 (realsecure), 445 (microsoft-ds), 80 (www), 27374 (SubSeven), 53 (domain) Source: http://isc.incidents.org/top10.html ; Internet Storm Center

[[Return to top](#)]

General Sector

24. *February 03, Associated Press* — **Southeast Asian terror network regrouping.** An al Qaeda-linked Southeast Asian terror network is regrouping with the help of porous borders, rising fanaticism, and new recruits, officials told The Associated Press ahead of an anti-terror conference. **Forced further underground by a police crackdown, dependent on couriers, and broken into isolated cells willing to lash out on their own, Jemaah Islamiyah (JI) is becoming less predictable, officials said.** "JI's capabilities have been degraded but they have certainly not been defeated," Australian Foreign Minister Alexander Downer said. **Cabinet ministers and other officials from 33 nations including U.S. Attorney General John Ashcroft meet Wednesday and Thursday to discuss expanding the anti-terror fight beyond the two-way agreements that have hurt but failed to defeat Jemaah Islamiyah.** Experts say Jemaah Islamiyah is now a very different group than the one blamed for killing 202 people by bombing Bali nightclubs in 2002. Officials say Jemaah Islamiyah's goal has remained unchanged: to establish an Islamic state in much of Southeast Asia. But with many of its leaders in jail and funds at a minimum, the fight is now increasingly waged by local cells, making their targets harder to predict, according to Indonesian police. **Jemaah Islamiyah has an estimated 2,000 operatives on the run throughout Southeast Asia.**
Source: http://abcnews.go.com/wire/World/ap20040203_1129.html

[[Return to top](#)]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web-site (<http://www.nipc.gov>), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings – DHS/IAIP Assessments, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications – DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive – Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions: nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703)883-3644

Subscription and Distribution Information Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703-883-3644 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call (202)323-3204.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open-source published information concerning significant critical infrastructure issues. This is an internal DHS/IAIP tool intended to serve the informational needs of DHS/IAIP personnel and other interested staff. Further reproduction or redistribution for private use or gain is subject to original copyright restrictions of the content. The IAIP provides no warranty of ownership of the copyright, or of accuracy in respect of the original source material.